



DELEGATING DIGITAL CREDENTIALSCROSS-REFERENCE TO RELATED APPLICATION

5           This application is a continuation-in-part of U.S.  
Patent Application No. 09/608,402, filed on June 30, 2000  
and entitled "Digital Credential Usage Reporting".

TECHNICAL FIELD

10           This invention relates to delegating digital  
credentials for use in accessing services.

BACKGROUND

15           Cryptography provides the basis for a number of privacy  
and authentication mechanisms used in computer-based  
systems. One such mechanism is a digital signature, which  
is often used to authenticate the sender of an electronic  
message. To create a digital signature, the sender first  
20       creates a private signature key and a corresponding public  
verification key. To sign a message or other document, the  
sender performs a computation that takes as input the  
message and the private signature key and produces as output  
a digital signature for that message. To verify a digital

signature, a receiver performs a computation that takes as input the message, the digital signature for that message, and the public verification key, and produces as output either "signature verified" or "signature failed to verify."

5           In order to facilitate the authentication of a digitally signed document, the receiver must be assured that the public verification key that is used to verify the signature is indeed the public verification key belonging to the sender of the message. Typically, the receiver will  
10 obtain a digital certificate, which contains the identity of the sender, the public verification key of the sender, and other information. Typically, this digital certificate is  
15 digitally signed by a certification authority. Other mechanisms are also used for establishing the correspondence between an identity and a public verification key such as an entry in a database.

#### DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating one example of a system that monitors the usage of digital credentials.

20           Figure 2 is a flow chart illustrating one example of a process for monitoring the usage of digital credentials.

Figure 3 is an example activity log.

Figure 4 is a block diagram illustrating a computer suitable for implementing embodiments of the invention.

Fig. 5 is a block diagram showing various elements of a delegation transaction.

5 Fig. 6 is a flowchart showing a process for delegating roles to a delegate.

Fig. 7 is a flowchart showing a process for selecting delegation credentials of a delegator.

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20

Fig. 8 is a flowchart showing a process for using a confirmation code in the delegation process.

#### DESCRIPTION

A user's "digital credential", as used herein, refers to the security mechanisms associated with the user's identity. For example, a user's digital credential can include one or more digital signature keys relating to one or more digital certificates. In addition, a user's digital credential can be any other suitable cryptographic security mechanism, such as a mechanism for use in a proprietary cryptographic scheme.

20 Validating a user's digital credential, therefore, can include one or more tasks. Examples include verifying that the user's digital signature is valid using the public key

in the user's digital certificate and validating the digital certificate, which can include several additional tasks such as using a key of the certification authority to validate that the digital signature on the digital certificate is valid, verifying that the digital certificate has not been revoked or suspended, and validating the key of the certification authority.

Figure 1 is a block diagram illustrating one example of a system 2 that tracks the usage of digital credentials, generates activity reports, and identifies potential fraudulent activities or other misuse. As explained in detail below, system 2 allows timely detection of fraudulent activity or general misuse of digital credentials.

Web browser 12, such as Internet Explorer™ from Microsoft™ Corporation of Redmond, Washington, executes in an operating environment provided by computing device 4A and allows an owner of digital credential 16 to remotely access online services 6 via network 28. Generally, online services 6 represent Web-based venues that support secure electronic transactions. For example, online services 6 can be Web-based retailers of consumer products such as books, movies, software, toys, games and the like. Alternatively, online services 6 can be business-to-business Web sites such

as online marketplaces for medical and other supplies. Other examples include online banking institutions, brokerage firms, and health care services. Similarly, authorized delegates of the user use Web browsers (not shown) executing on computing devices 4B through 4M to access online services 6 and conduct secure transactions using a digital credential that has been authorized by the user to act on behalf of the user for specified uses.

Computing devices 4 represents general purpose computing systems suitable for interacting with network 28. One example of a suitable computing device 4 is a personal computer. In addition, each computing device 4 can be a laptop computer, a handheld computer, a personal digital assistant (PDA), such as a Palm™ organizer from Palm Inc. of Santa Clara, California, or even a network-enabled cellular telephone. Network 28 represents any communication network, such as a packet-based digital network like the Internet.

Credential service provider (CSP) 8 provides a central service by which a user can manage his or her digital credentials. More specifically, CSP 8 allows a user to request a digital credential, revoke a digital credential and define one or more delegates that are authorized to use

their own digital credential to act in behalf of the user for specified functions.

In order to obtain digital credential 16, the user directs Web browser 12 to CSP 8, generates a private signature key and a public verification key, and requests a digital certificate. The user submits the public verification key and a variety of information, such as name and address, that is validated during the application process.

CSP 8 submits the information to credential issuing service (CIS) 22 that, as a certificate authority, issues a corresponding digital credential 16, including a digital certificate and signature key, and records the owner information in owner database 24. In this fashion, the user becomes the "owner" of his or her digital credential 16. After CIS 22 issues digital credential 16 the owner can access CSP 8 and designate one or more authorized delegates.

The owner uses digital credential 16 to securely access online services 6, present digitally signed documents and otherwise conduct secure transactions. In one configuration, Web browser 12 establishes a secure communication link with a Web server at one of the online services 6 using a secure communications protocol, such as

the Secure Socket Layer (SSL). When accessed, the Web server issues a "challenge" to Web browser 12. Web browser 12 responds by signing the challenge with his private signature key and communicating digital credential 16 and the signed challenge to online service 6. In another configuration, Web browser 12 uses his private signature key to digitally sign a document presented to online server 6, such as when the owner or delegate is submitting a confidential medical diagnosis or a prescription request to a Web-based health care service.

Online services 6 can opt to validate digital credential 16 directly, such as by verifying the digital signatures using the public key and by checking a local database to verify the association between the public key and the user. However, online services 6 can also communicate the digital credential 16 to credential verification service 10 (CVS) for verification. In one configuration, online services 6 validate transactions of low monetary value locally and use CVS 10 to validate high value transactions.

To validate a digital credential 16, CVS 10 receives the digital credential, such as the digital signature and the digital certificate, from online services 6 and



interacts with CIS 22. CVS 10 accesses CIS 22 to obtain the public key for CIS 22, as a certificate authority, and verifies the digital signature. Next, CVS 20 accesses CIS 22 to determine whether digital credential 16 has been  
5 revoked, as indicated by certificate repository 26. CVS 20 stores the result of the verification, whether successful or not, in activity log 20.

In one configuration, CSP 8 allows the user to generate a number of digital signature keys associated with his  
10 identity and assign a "friendly name" to each key. For example, the user may assign names such as: Office Key, Home Key, Portable Key. As described below, this allows the user to more readily track usage of the digital signature keys.

System 2 incorporates many features that allow an owner  
15 or delegate to detect unauthorized use of the digital signature key in the event digital signature key is misappropriated or otherwise misused. For example, when verifying digital signature during each secure transaction, CVS 10 can automatically send an activity report to Web  
20 browser 12, which can display the activity report to the user. In this fashion the user can readily identify whether the digital signature key is being misused.

In addition, the owner or delegate can access CSP 8 and request an activity report that details any usage of digital signature key. Upon receiving such a request, CSP 8 communicates the request directly to CVS 10. CVS 10 examines activity log 20, extracts the relevant activity information, formulates a report and communicates the report to CSP 8. CSP 8 electronically presents the report to the user via network 28. The owner or delegate can also configure CSP 8 to periodically generate the report and electronically mail the report to the user. Alternatively, CSP 8 can mail a physical copy of the report to the user.

In addition to the above-described techniques by which an owner or delegate can detect misuse of digital credential, fraud detection module 18 of CVS 10 applies fraud detection techniques to activity log 20 in order to automatically identify misuse. As described in detail below, fraud detection module 18 analyzes activity log 20 to identify any unusual patterns that may indicate misuse.

Figure 2 is a flow chart illustrating a process 30 further illustrating how system 2 monitors the usage of digital signature keys and identifies potential fraudulent activities or general misuse. Each online service 6 processes secure transactions by communicating digital

credential 16 to CVS 10 for verification (32). As described above, CVS 10 cooperates with CIS 22 to verify digital credential 16 including determining whether digital credential 16 is revoked. In one configuration, however, 5 online services validate the digital credential and communicate transaction information to CVS 10.

CVS 10 stores the result of each verification in activity log 26 (34). In addition, CVS 10 stores relevant transaction information such as a date and time of the transaction, the online service 6 that is involved in the transaction, the type of transaction, the device used to access the online service 6, such as a laptop computer, cell phone or a PDA, the value of the transaction, and location and position information, such as an IP address or a name of computing device 4. 15

In order to facilitate the timely identification of misuse of digital credential 16, CVS 10 generates activity reports that detail the information stored in activity log 20 (36). As discussed above, CVS 10 generates the activity reports in a variety of ways and at a variety of times. For 20 example, CVS 10 can automatically generate an activity report when handling each verification request, thereby frequently providing the information to the user. In

addition, CVS 10 can periodically generate activity reports or upon request by the owner.

CVS 10 also tailors each activity report to the requestor such that the owner of digital credential 16 can view all activity, including any activity by the delegates. An individual delegate, however, can only view activity reports that list his or her activity.

Fraud detection module 18 of CVS 10 analyzes activity log 20 to identify any unusual patterns in order to identify fraudulent activities. For example, a significant increase in the number or the size of the transactions can indicate misuse. A change in the types of transactions can indicate misuse. In addition, any indication that digital signature key 16 is suddenly being used from a different computing device, such as a change from a frequently used internet protocol (IP) address to a previously unused IP address, can also indicate misuse. Upon detecting potential misuse, CVS 10 communicates an activity report to the owner alerting him or her of the activity. In this manner, the owner can readily determine whether any fraudulent activity or general misuse has indeed occurred and the extent of the activity.

If the owner determines that unauthorized activities have indeed occurred, the owner can access CSP 8 and revoke

digital credential 16. For example, the owner can revoke the associated digital certificate. Alternatively, the owner can create a new private signature key and a new public verification key and sign this public verification key with the old private signature key. System 2 can issue a new digital certificate for this new verification key. CSP 8 communicates the revocation to CIS 22, which updates the status of digital credential 16 in certificate repository 26, thereby causing any future verifications by CVS 10 of the digital credential to fail. Thus, the owner can immediately stop the fraudulent activity.

In addition, the activity report can be provided to an authorized operator of CSP 8 of CVS 10. Furthermore, an activity report detailing activity at a specific online service 6 can be generated and provided to an authorized operator at the online service.

It this manner, system 2 helps detect unauthorized use of the digital signature key in the event digital signature key is misappropriated. These features are especially advantages to professional services such as the healthcare profession. To further illustrate these benefits, consider a healthcare professional accessing a healthcare oriented online service and requesting access to healthcare

information or seeking to submit a prescriptions or  
diagnosis. The online service communicates transaction  
information describing the access request and the medical  
professional's digital credential to the central credential  
5 verification service. Upon receiving a verification result  
from the credential verification service, the healthcare  
oriented service provides access to the medical records.  
Subsequently, the healthcare oriented service receives an  
activity report from the credential verification service and  
provides the report to healthcare professional.

Figure 3 is an example activity report 40 generated by  
CVS 10. Activity report 40 lists the activities logged in  
activity log 20, broken down by owner and delegate. For  
each authentication request, the example activity report 40  
15 lists the date and time, the online service involved in the  
transaction, the name of the computing device 4 used by the  
user to originate the transaction, the value of the  
transaction, the type of the transaction, and the  
authentication result.

20 Figure 4 illustrates a programmable computing system  
(system) 100 that provides an operating environment suitable  
for use as a computing device 4 or as a server within CSP 8,  
CVS 10 or CIS 22. The system 100 includes a processor 112

that represents any suitable microprocessor such as the PENTIUM® family of microprocessors manufactured by the Intel Corporation of Santa Clara, California. Other examples include the MIPS® family of microprocessors, the POWERPC® family of microprocessors from both the Motorola Corporation and the IBM Corporation, the PRECISION ARCHITECTURE® family of microprocessors from the Hewlett-Packard Company, the SPARC® family of microprocessors from the Sun Microsystems Corporation, or the ALPHA® family of microprocessors from the Compaq Computer Corporation. In various configurations, system 100 represents any server, personal computer, laptop or a hand-held PC, a personal digital assistant (PDA) or a network-enabled cellular phone.

System 100 includes system memory 113, including read only memory (ROM) 114 and random access memory (RAM) 115, which is connected to the processor 112 by a system data/address bus 116. Input/output bus 118 is connected to the data/address bus 116 via bus controller 119. In one embodiment, input/output bus 118 is implemented as a standard Peripheral Component Interconnect (PCI) bus. The bus controller 119 examines all signals from the processor 112 to route the signals to the appropriate bus. Signals between the processor 112 and the system memory 113 are

merely passed through the bus controller 119. However, signals from the processor 112 intended for devices other than system memory 113 are routed onto the input/output bus 118.

5           Various devices are connected to the input/output bus 118 including hard disk drive 120, floppy drive 121 that is used to read floppy disk 151, and optical drive 122, such as a CD-ROM drive that is used to read an optical disk 152. The video display 124 or other kind of display device is connected to the input/output bus 118 via a video adapter 125.

10           Users enter commands and information into the system 100 by using a keyboard 140 and/or pointing device, such as a mouse 142, which are connected to bus 118 via input/output ports 128. Other types of pointing devices (not shown) include track pads, track balls, joysticks, data gloves, head trackers, and other devices suitable for positioning a cursor on the video display 124. System 100 also includes a modem 129 that is typically used to communicate over wide  
15           area networks (not shown), such as the Internet using either  
20           a wired or wireless connection.

          Software applications 136 and data are typically stored via one of the memory storage devices, which may include the



hard disk 120, floppy disk 151, CD-ROM 152 and are copied to RAM 115 for execution. In one embodiment, however, software applications 136 are stored in ROM 114 and are copied to RAM 115 for execution or are executed directly from ROM 114.

5 In general, the operating system 135 executes software applications 136 and carries out instructions issued by the user. The Basic Input/Output System (BIOS) 117 for the system 100 is a set of basic executable routines that have conventionally helped to transfer information between the computing resources within the system 100. Operating system 135 or other software applications 136 use these low-level service routines. In one embodiment system 100 includes a registry (not shown) that is a system database that holds configuration information for system 100.

10 CVS 10 and CIS 22 may be implemented within the same machine (e.g., computer) as CSP 8 or in separate machines (as shown). The following description assumes that they are all implemented within the same machine.

## 20 Delegating Roles

In this embodiment, a delegator, e.g., an owner of a digital credential, can delegate a role or function to a delegate. That is, the delegator need not delegate all of

his or her authority to the delegate, but rather a subset thereof. For example, a doctor may delegate to a secretary the ability to view a patient's medical records relating to billing, but not those relating to diagnosis. The same  
5 doctor may also delegate to an X-ray technician that same patient's medical records relating to diagnosis, but not to billing. Thus, the doctor is able to delegate partial authority to different types of assistants, without delegating his full authority to anyone.

10 "Delegation credentials" are a type of digital credential (defined above) that allow the delegator to delegate only some functions or authority to a delegate. The delegation credentials define one or more delegates that are authorized to use a delegator's digital credential to  
15 act on behalf of the delegator for specified functions.

Referring to Fig. 5, a block diagram is shown which indicates the various elements of a delegation transaction. These elements include a delegator 200, a delegate 202, a relying party 204, a CSP 206, and a delegation service  
20 provider (DSP) 208. Each of these elements may be implemented using a programmable computing system, such as system 100 shown in Fig. 4 (the delegator and delegate may be entities who may use a system 100).

Delegator 200 is an entity, such as a person, company, etc., who delegates one or more functions to a delegate 202. Delegate 202 receives the authority to perform those functions using delegation credentials, as described below.

5 Relying party 204 is an entity that provides a requested service in reliance on the delegated credentials of the delegate. For example, relying party 204 may be a Web site that receives delegation credentials (of the delegator) from the delegate and, once they are verified, provides the delegate with access to services (e.g., information) that was previously available only to the delegator.

CSP 206 is as described above and, for the purposes of this embodiment, includes a CVS and CIS. In this regard, CSP 206 maintains access to a database 210 that contains delegation credentials of the delegator and a database 212 that contains activity logs that store information such as which delegation credentials have been delegated to which delegate. Although databases 210 and 212 are shown separately in Fig. 5, they may be a single database.

20 DSP 208 controls the delegation of delegation credentials to delegates. To this end, DSP 208 maintains a database 214 of delegation information, which identifies delegators, delegates, the functions available to the

delegators, and which of those functions, if any, are available to the delegates. DSP 208 and CSP 206 are shown as separate machines in Fig. 5; however, they may be implemented using the same machine.

5 Referring to Fig. 6, a process 216 is shown for providing a delegate with the authority to assume one or more roles of a delegator. Referring to Figs. 5 and 6, the delegator registers (218) for a digital credential with CSP 206. The delegator provides registration information, such as his identity, professional title, authority, etc. to CSP 206. CSP 206 may contain a database of information about potential subscribers, such as delegator 200. Once delegator 200 enters the registration information, CSP 206 may check (220) the registration information against (e.g., compare it to) information in the database. If there is sufficient correspondence between the registration information and the information stored in the database, CSP 206 may issue (220) a digital credential to delegator 200. It is noted that the checking may be bypassed and CSP 206 may simply issue (220) the digital credential upon receipt of the registration information and, e.g., payment.

Delegator 200 may then delegate one or more roles (e.g., professional titles, authority, functions) to a

delegate. To do this, delegator 200 provides DSP 208 with a designation, which includes a role and a delegate to assume the role. Delegator 200 approves the designation using the digital credential that the delegator received during registration. Delegator 200 provides the designation and the digital credential to CSP 206. CSP 206 confirms that the designation did indeed come from the delegator by verifying the delegator's digital credential and informs DSP 208 that the designation is valid. CSP 206 also logs the designation and its approval in database 212.

DSP 208 receives (222) the designation (including the identity of the delegate and role(s)) from delegator 200 and receives the approval from CSP 206. In response to the approval, DSP 208 issues (226) a delegation credential. The delegation credential may be issued (226) directly to the delegator or it may be issued to CSP 206, which will, in turn, provide it to the delegator or to any third party, as needed, where it is stored. The delegation credential contains delegation information, such as the identity of the delegate and the role(s) of the delegator that the delegate may assume.

DSP 208 may store the delegation credential in database 214, along with an indication that the initial designation

was approved. DSP 208 may also send (228) a confirmation message to delegator 200 indicating that the requested delegation was created.

Referring to Fig. 7, a process 230 is shown in which a  
5 delegate uses delegation credentials to access services available to the delegator from a relying party. Delegate 202 requests (232), from a relying party 204 such as a Web site, access to a service that requires a digital credential. In response to the request, relying party 204  
10 sends an access request to the delegate to be approved by a digital credential. The delegate sends a delegation credential in response. CSP 206 receives (234) the delegation credential from the delegate and the access requirements from relying party 204.

CSP 206 determines (236) if the delegation credential  
15 is valid for the access requirement. What this means is that CSP 206 determines if, based on the delegation credential, the delegate may access the services of relying party 204. CSP 206 also confirms that the delegation  
20 credential is valid by comparing it to stored delegation credentials.

If the delegation credential is valid for the access requirement, CSP 206 informs (238) relying party 204 that

the delegation credential is valid. If the delegation credential is not valid for the access requirement, CSP 206 obtains (240) the delegation credentials available to the delegate (e.g., from database 210) and determines (240) if there is a delegation credential that corresponds to the access requirement. If there is more than one delegation credential that is available to the delegate that will satisfy the access requirements of the relying party, CSP 206 provides (242) a list of those delegation credentials to the delegate. The delegate may then select (244), from the list, which of the delegation credentials to use. If no delegation is found, CSP 206 informs relying party 204 that no appropriate delegation is available.

The selected delegation credential may be sent to a verification service, such as a CVS within CSP 206. The verification service compares the delegation credential to a list of permissible delegation credentials for the delegate. If the delegation credential is verified, e.g., it is on the list, the verification service logs that the delegation credential is to be used for access to the service of the relying party and signs a digital statement asserting the validity of the delegation credential for the requested

access. The digital statement may be provided to relying party 204.

CSP 206 and relying party 204 receive an indication of which of the delegation credentials the delegate has selected, along with the verification service statement (if applicable). The delegation credential is then used (246) to provide access to the requested service. That is, relying party 204 verifies the verification statement and/or delegation credential and, once verified, provides the requested service to the delegate.

CSP 206 logs the identity of the delegation credential that the delegate uses to access the services of relying party 204. The logs that are kept by CSP 206 may be made available to the delegate and/or the delegator to examine. Thus, the delegator can view all activities that the delegate took on his behalf or reports of such activities. If the delegator (or delegate) finds that an inappropriate action has been taken, he may revoke the delegation credential under which that action was taken. This can be done by communicating a revocation request to DSP 208 and/or CSP 206. Using the stored logs, a delegator is also able to review all of the delegation credentials that he created in order to detect if any were created fraudulently. The



delegator is also able to review the delegation credentials created on his behalf by a delegate, if such creation is permitted in the first place.

In other embodiments, DSP 208 could send all of the delegation credentials of the delegate to the relying party and then have the relying party check to see if there are any delegation credentials that satisfy its access requirements. The delegate could store the delegation information instead of, or in addition to, storage on DSP 208. The delegate could then provide this information to the relying party when the delegate requests a service.

The delegate could have a default delegation credential. When multiple delegation credentials meet the access requirements of the relying party, the delegate could be presented with a graphical user interface that includes the default delegation credential pre-selected. The delegate could then just accept the default delegation.

DSP 208 could also send all of the delegation credentials of the delegate to the relying party and then have the relying party check whether there are any delegation credentials that satisfy its access requirements.

Referring to Fig. 8, a process 248 is shown in which a confirmation code is used to assign a delegation credential

to a delegate. Process 248 may be used, for example, in blocks 226 and 228 of process 216 (Fig. 6).

In process 248, a delegator decides to assign a delegation. To do this, the delegator may visit a delegation Web site (not shown) and select the roles that are to be assigned to the delegate. For example, the delegator may select, from the Web site, professional titles, such as secretary, technician, etc., that define the roles. The delegator then provides (e.g., via the Web site) a confirmation code. The confirmation code may be a random N-digit alphanumeric sequence (where  $N > 1$ ). The Web site may hash the confirmation code using a cryptographic hash function, such as SHA-1. The delegator approves the selected roles and confirmation code (hashed or non-hashed) using his digital credential. DSP 206 receives the confirmation code or hashed confirmation code.

DSP 208 receives the confirmation code, the selected roles, and an identifier for the delegator. The identifier may be a name or number that corresponds to, e.g., identifies, the delegator. DSP 208 stores this information in database 214. The delegator provides the confirmation code and the identifier to the delegate. This information may be provided by hand, electronic mail, or some other

secure method that is independent of the delegation processes described herein.

The delegate enters the identifier and the confirmation code into an appropriate area of the delegation Web site.

5 DSP 208 receives (250) the identifier and the confirmation code from the Web site and identifies (252) the delegator using this information. This may be done by comparing the identifier to a pre-stored identifier for the delegator and/or checking the hash of the confirmation code for correctness. DSP 208 may then assign (254) the appropriate delegation credential(s) to the delegate and send (256) a confirmation of the delegation to the delegator.

10  
15  
20  
25  
30  
35  
40  
45  
50  
55  
60  
65  
70  
75  
80  
85  
90  
95  
100  
105  
110  
115  
120  
125  
130  
135  
140  
145  
150  
155  
160  
165  
170  
175  
180  
185  
190  
195  
200  
205  
210  
215  
220  
225  
230  
235  
240  
245  
250  
255  
260  
265  
270  
275  
280  
285  
290  
295  
300  
305  
310  
315  
320  
325  
330  
335  
340  
345  
350  
355  
360  
365  
370  
375  
380  
385  
390  
395  
400  
405  
410  
415  
420  
425  
430  
435  
440  
445  
450  
455  
460  
465  
470  
475  
480  
485  
490  
495  
500  
505  
510  
515  
520  
525  
530  
535  
540  
545  
550  
555  
560  
565  
570  
575  
580  
585  
590  
595  
600  
605  
610  
615  
620  
625  
630  
635  
640  
645  
650  
655  
660  
665  
670  
675  
680  
685  
690  
695  
700  
705  
710  
715  
720  
725  
730  
735  
740  
745  
750  
755  
760  
765  
770  
775  
780  
785  
790  
795  
800  
805  
810  
815  
820  
825  
830  
835  
840  
845  
850  
855  
860  
865  
870  
875  
880  
885  
890  
895  
900  
905  
910  
915  
920  
925  
930  
935  
940  
945  
950  
955  
960  
965  
970  
975  
980  
985  
990  
995  
1000  
1005  
1010  
1015  
1020  
1025  
1030  
1035  
1040  
1045  
1050  
1055  
1060  
1065  
1070  
1075  
1080  
1085  
1090  
1095  
1100  
1105  
1110  
1115  
1120  
1125  
1130  
1135  
1140  
1145  
1150  
1155  
1160  
1165  
1170  
1175  
1180  
1185  
1190  
1195  
1200  
1205  
1210  
1215  
1220  
1225  
1230  
1235  
1240  
1245  
1250  
1255  
1260  
1265  
1270  
1275  
1280  
1285  
1290  
1295  
1300  
1305  
1310  
1315  
1320  
1325  
1330  
1335  
1340  
1345  
1350  
1355  
1360  
1365  
1370  
1375  
1380  
1385  
1390  
1395  
1400  
1405  
1410  
1415  
1420  
1425  
1430  
1435  
1440  
1445  
1450  
1455  
1460  
1465  
1470  
1475  
1480  
1485  
1490  
1495  
1500  
1505  
1510  
1515  
1520  
1525  
1530  
1535  
1540  
1545  
1550  
1555  
1560  
1565  
1570  
1575  
1580  
1585  
1590  
1595  
1600  
1605  
1610  
1615  
1620  
1625  
1630  
1635  
1640  
1645  
1650  
1655  
1660  
1665  
1670  
1675  
1680  
1685  
1690  
1695  
1700  
1705  
1710  
1715  
1720  
1725  
1730  
1735  
1740  
1745  
1750  
1755  
1760  
1765  
1770  
1775  
1780  
1785  
1790  
1795  
1800  
1805  
1810  
1815  
1820  
1825  
1830  
1835  
1840  
1845  
1850  
1855  
1860  
1865  
1870  
1875  
1880  
1885  
1890  
1895  
1900  
1905  
1910  
1915  
1920  
1925  
1930  
1935  
1940  
1945  
1950  
1955  
1960  
1965  
1970  
1975  
1980  
1985  
1990  
1995  
2000  
2005  
2010  
2015  
2020  
2025  
2030  
2035  
2040  
2045  
2050  
2055  
2060  
2065  
2070  
2075  
2080  
2085  
2090  
2095  
2100  
2105  
2110  
2115  
2120  
2125  
2130  
2135  
2140  
2145  
2150  
2155  
2160  
2165  
2170  
2175  
2180  
2185  
2190  
2195  
2200  
2205  
2210  
2215  
2220  
2225  
2230  
2235  
2240  
2245  
2250  
2255  
2260  
2265  
2270  
2275  
2280  
2285  
2290  
2295  
2300  
2305  
2310  
2315  
2320  
2325  
2330  
2335  
2340  
2345  
2350  
2355  
2360  
2365  
2370  
2375  
2380  
2385  
2390  
2395  
2400  
2405  
2410  
2415  
2420  
2425  
2430  
2435  
2440  
2445  
2450  
2455  
2460  
2465  
2470  
2475  
2480  
2485  
2490  
2495  
2500  
2505  
2510  
2515  
2520  
2525  
2530  
2535  
2540  
2545  
2550  
2555  
2560  
2565  
2570  
2575  
2580  
2585  
2590  
2595  
2600  
2605  
2610  
2615  
2620  
2625  
2630  
2635  
2640  
2645  
2650  
2655  
2660  
2665  
2670  
2675  
2680  
2685  
2690  
2695  
2700  
2705  
2710  
2715  
2720  
2725  
2730  
2735  
2740  
2745  
2750  
2755  
2760  
2765  
2770  
2775  
2780  
2785  
2790  
2795  
2800  
2805  
2810  
2815  
2820  
2825  
2830  
2835  
2840  
2845  
2850  
2855  
2860  
2865  
2870  
2875  
2880  
2885  
2890  
2895  
2900  
2905  
2910  
2915  
2920  
2925  
2930  
2935  
2940  
2945  
2950  
2955  
2960  
2965  
2970  
2975  
2980  
2985  
2990  
2995  
3000  
3005  
3010  
3015  
3020  
3025  
3030  
3035  
3040  
3045  
3050  
3055  
3060  
3065  
3070  
3075  
3080  
3085  
3090  
3095  
3100  
3105  
3110  
3115  
3120  
3125  
3130  
3135  
3140  
3145  
3150  
3155  
3160  
3165  
3170  
3175  
3180  
3185  
3190  
3195  
3200  
3205  
3210  
3215  
3220  
3225  
3230  
3235  
3240  
3245  
3250  
3255  
3260  
3265  
3270  
3275  
3280  
3285  
3290  
3295  
3300  
3305  
3310  
3315  
3320  
3325  
3330  
3335  
3340  
3345  
3350  
3355  
3360  
3365  
3370  
3375  
3380  
3385  
3390  
3395  
3400  
3405  
3410  
3415  
3420  
3425  
3430  
3435  
3440  
3445  
3450  
3455  
3460  
3465  
3470  
3475  
3480  
3485  
3490  
3495  
3500  
3505  
3510  
3515  
3520  
3525  
3530  
3535  
3540  
3545  
3550  
3555  
3560  
3565  
3570  
3575  
3580  
3585  
3590  
3595  
3600  
3605  
3610  
3615  
3620  
3625  
3630  
3635  
3640  
3645  
3650  
3655  
3660  
3665  
3670  
3675  
3680  
3685  
3690  
3695  
3700  
3705  
3710  
3715  
3720  
3725  
3730  
3735  
3740  
3745  
3750  
3755  
3760  
3765  
3770  
3775  
3780  
3785  
3790  
3795  
3800  
3805  
3810  
3815  
3820  
3825  
3830  
3835  
3840  
3845  
3850  
3855  
3860  
3865  
3870  
3875  
3880  
3885  
3890  
3895  
3900  
3905  
3910  
3915  
3920  
3925  
3930  
3935  
3940  
3945  
3950  
3955  
3960  
3965  
3970  
3975  
3980  
3985  
3990  
3995  
4000  
4005  
4010  
4015  
4020  
4025  
4030  
4035  
4040  
4045  
4050  
4055  
4060  
4065  
4070  
4075  
4080  
4085  
4090  
4095  
4100  
4105  
4110  
4115  
4120  
4125  
4130  
4135  
4140  
4145  
4150  
4155  
4160  
4165  
4170  
4175  
4180  
4185  
4190  
4195  
4200  
4205  
4210  
4215  
4220  
4225  
4230  
4235  
4240  
4245  
4250  
4255  
4260  
4265  
4270  
4275  
4280  
4285  
4290  
4295  
4300  
4305  
4310  
4315  
4320  
4325  
4330  
4335  
4340  
4345  
4350  
4355  
4360  
4365  
4370  
4375  
4380  
4385  
4390  
4395  
4400  
4405  
4410  
4415  
4420  
4425  
4430  
4435  
4440  
4445  
4450  
4455  
4460  
4465  
4470  
4475  
4480  
4485  
4490  
4495  
4500  
4505  
4510  
4515  
4520  
4525  
4530  
4535  
4540  
4545  
4550  
4555  
4560  
4565  
4570  
4575  
4580  
4585  
4590  
4595  
4600  
4605  
4610  
4615  
4620  
4625  
4630  
4635  
4640  
4645  
4650  
4655  
4660  
4665  
4670  
4675  
4680  
4685  
4690  
4695  
4700  
4705  
4710  
4715  
4720  
4725  
4730  
4735  
4740  
4745  
4750  
4755  
4760  
4765  
4770  
4775  
4780  
4785  
4790  
4795  
4800  
4805  
4810  
4815  
4820  
4825  
4830  
4835  
4840  
4845  
4850  
4855  
4860  
4865  
4870  
4875  
4880  
4885  
4890  
4895  
4900  
4905  
4910  
4915  
4920  
4925  
4930  
4935  
4940  
4945  
4950  
4955  
4960  
4965  
4970  
4975  
4980  
4985  
4990  
4995  
5000  
5005  
5010  
5015  
5020  
5025  
5030  
5035  
5040  
5045  
5050  
5055  
5060  
5065  
5070  
5075  
5080  
5085  
5090  
5095  
5100  
5105  
5110  
5115  
5120  
5125  
5130  
5135  
5140  
5145  
5150  
5155  
5160  
5165  
5170  
5175  
5180  
5185  
5190  
5195  
5200  
5205  
5210  
5215  
5220  
5225  
5230  
5235  
5240  
5245  
5250  
5255  
5260  
5265  
5270  
5275  
5280  
5285  
5290  
5295  
5300  
5305  
5310  
5315  
5320  
5325  
5330  
5335  
5340  
5345  
5350  
5355  
5360  
5365  
5370  
5375  
5380  
5385  
5390  
5395  
5400  
5405  
5410  
5415  
5420  
5425  
5430  
5435  
5440  
5445  
5450  
5455  
5460  
5465  
5470  
5475  
5480  
5485  
5490  
5495  
5500  
5505  
5510  
5515  
5520  
5525  
5530  
5535  
5540  
5545  
5550  
5555  
5560  
5565  
5570  
5575  
5580  
5585  
5590  
5595  
5600  
5605  
5610  
5615  
5620  
5625  
5630  
5635  
5640  
5645  
5650  
5655  
5660  
5665  
5670  
5675  
5680  
5685  
5690  
5695  
5700  
5705  
5710  
5715  
5720  
5725  
5730  
5735  
5740  
5745  
5750  
5755  
5760  
5765  
5770  
5775  
5780  
5785  
5790  
5795  
5800  
5805  
5810  
5815  
5820  
5825  
5830  
5835  
5840  
5845  
5850  
5855  
5860  
5865  
5870  
5875  
5880  
5885  
5890  
5895  
5900  
5905  
5910  
5915  
5920  
5925  
5930  
5935  
5940  
5945  
5950  
5955  
5960  
5965  
5970  
5975  
5980  
5985  
5990  
5995  
6000  
6005  
6010  
6015  
6020  
6025  
6030  
6035  
6040  
6045  
6050  
6055  
6060  
6065  
6070  
6075  
6080  
6085  
6090  
6095  
6100  
6105  
6110  
6115  
6120  
6125  
6130  
6135  
6140  
6145  
6150  
6155  
6160  
6165  
6170  
6175  
6180  
6185  
6190  
6195  
6200  
6205  
6210  
6215  
6220  
6225  
6230  
6235  
6240  
6245  
6250  
6255  
6260  
6265  
6270  
6275  
6280  
6285  
6290  
6295  
6300  
6305  
6310  
6315  
6320  
6325  
6330  
6335  
6340  
6345  
6350  
6355  
6360  
6365  
6370  
6375  
6380  
6385  
6390  
6395  
6400  
6405  
6410  
6415  
6420  
6425  
6430  
6435  
6440  
6445  
6450  
6455  
6460  
6465  
6470  
6475  
6480  
6485  
6490  
6495  
6500  
6505  
6510  
6515  
6520  
6525  
6530  
6535  
6540  
6545  
6550  
6555  
6560  
6565  
6570  
6575  
6580  
6585  
6590  
6595  
6600  
6605  
6610  
6615  
6620  
6625  
6630  
6635  
6640  
6645  
6650  
6655  
6660  
6665  
6670  
6675  
6680  
6685  
6690  
6695  
6700  
6705  
6710  
6715  
6720  
6725  
6730  
6735  
6740  
6745  
6750  
6755  
6760  
6765  
6770  
6775  
6780  
6785  
6790  
6795  
6800  
6805  
6810  
6815  
6820  
6825  
6830  
6835  
6840  
6845  
6850  
6855  
6860  
6865  
6870  
6875  
6880  
6885  
6890  
6895  
6900  
6905  
6910  
6915  
6920  
6925  
6930  
6935  
6940  
6945  
6950  
6955  
6960  
6965  
6970  
6975  
6980  
6985  
6990  
6995  
7000  
7005  
7010  
7015  
7020  
7025  
7030  
7035  
7040  
7045  
7050  
7055  
7060  
7065  
7070  
7075  
7080  
7085  
7090  
7095  
7100  
7105  
7110  
7115  
7120  
7125  
7130  
7135  
7140  
7145  
7150  
7155  
7160  
7165  
7170  
7175  
7180  
7185  
7190  
7195  
7200  
7205  
7210  
7215  
7220  
7225  
7230  
7235  
7240  
7245  
7250  
7255  
7260  
7265  
7270  
7275  
7280  
7285  
7290  
7295  
7300  
7305  
7310  
7315  
7320  
7325  
7330  
7335  
7340  
7345  
7350  
7355  
7360  
7365  
7370  
7375  
7380  
7385  
7390  
7395  
7400  
7405  
7410  
7415  
7420  
7425  
7430  
7435  
7440  
7445  
7450  
7455  
7460  
7465  
7470  
7475  
7480  
7485  
7490  
7495  
7500  
7505  
7510  
7515  
7520  
7525  
7530  
7535  
7540  
7545  
7550  
7555  
7560  
7565  
7570  
7575  
7580  
7585  
7590  
7595  
7600  
7605  
7610  
7615  
7620  
7625  
7630  
7635  
7640  
7645  
7650  
7655  
7660  
7665  
7670  
7675  
7680  
7685  
7690  
7695  
7700  
7705  
7710  
7715  
7720  
7725  
7730  
7735  
7740  
7745  
7750  
7755  
7760  
7765  
7770  
7775  
7780  
7785  
7790  
7795  
7800  
7805  
7810  
7815  
7820  
7825  
7830  
7835  
7840  
7845  
7850  
7855  
7860  
7865  
7870  
7875  
7880  
7885  
7890  
7895  
7900  
7905  
7910  
7915  
7920  
7925  
7930  
7935  
7940  
7945  
7950  
7955  
7960  
7965  
7970  
7975  
7980  
7985  
7990  
7995  
8000  
8005  
8010  
8015  
8020  
8025  
8030  
8035  
8040  
8045  
8050  
8055  
8060  
8065  
8070  
8075  
8080  
8085  
8090  
8095  
8100  
8105  
8110  
8115  
8120  
8125  
8130  
8135  
8140  
8145  
8150  
8155  
8160  
8165  
8170  
8175  
8180  
8185  
8190  
8195  
8200  
8205  
8210  
8215  
8220  
8225  
8230  
8235  
8240  
8245  
8250  
8255  
8260  
8265  
8270  
8275  
8280  
8285  
8290  
8295  
8300  
8305  
8310  
8315  
8320  
8325  
8330  
8335  
8340  
8345  
8350  
8355  
8360  
8365  
8370  
8375  
8380  
8385  
8390  
8395  
8400  
8405  
8410  
8415  
8420  
8425  
8430  
8435  
8440  
8445  
8450  
8455  
8460  
8465  
8470  
8475  
8480  
8485  
8490  
8495  
8500  
8505  
8510  
8515  
8520  
8525  
8530  
8535  
8540  
8545  
8550  
8555  
8560  
8565  
8570  
8575  
8580  
8585  
8590  
8595  
8600  
8605  
8610  
8615  
8620  
8625  
8630  
8635  
8640  
8645  
8650  
8655  
8660  
8665  
8670  
8675  
8680  
8685  
8690  
8695  
8700  
8705  
8710  
8715  
8720  
8725  
8730  
8735  
8740  
8745  
8750  
8755  
8760  
8765  
8770  
8775  
8780  
8785  
8790  
8795  
8800  
8805  
8810  
8815  
8820  
8825  
8830  
8835  
8840  
8845  
8850  
8855  
8860  
8865  
8870  
8875  
8880  
8885  
8890  
8895  
8900  
8905  
8910  
8915  
8920  
8925  
8930  
8935  
8940  
8945  
8950  
8955  
8960  
8965  
8970  
8975  
8980  
8985  
8990  
8995  
9000  
9005  
9010  
9015  
9020  
9025  
9030  
9035  
9040  
9045  
9050  
9055  
9060  
9065  
9070  
9075  
9080  
9085  
9090  
9095  
9100  
9105  
9110  
9115  
9120  
9125  
9130  
9135  
9140  
9145  
9150  
9155  
9160  
9165  
9170  
9175  
9180  
9185  
9190  
9195  
9200  
9205  
9210  
9215  
9220  
9225  
9230  
9235  
9240  
9245  
9250  
9255  
9260  
9265  
9270  
9275  
9280  
9285  
9290  
9295  
9300  
9305  
9310  
9315  
9320  
9325  
9330  
9335  
9340  
9345  
9350  
9355  
9360  
9365  
9370  
9375  
9380  
9385  
9390  
9395  
9400  
9405  
9410  
9415  
9420  
9425  
9430  
9435  
9440  
9445  
9450  
9455  
9460  
9465  
9470  
9475  
9480  
9485  
9490  
9495  
9500  
9505  
9510  
9515  
9520  
9525  
9530  
9535  
9540  
9545  
9550  
9555  
9560  
9565  
9570  
9575  
9580  
9585  
9590  
9595  
9600  
9605  
9610  
9615  
9620  
9625  
9630  
9635  
9640  
9645  
9650  
9655  
9660  
9665  
9670  
9675  
9680  
9685  
9690  
9695  
9700  
9705  
9710  
9715  
9720  
9725  
9730  
9735  
9740  
9745  
9750  
9755  
9760  
9765  
9770  
9775  
9780  
9785  
9790  
9795  
9800  
9805  
9810  
9815  
9820  
9825  
9830  
9835  
9840  
9845  
9850  
9855  
9860  
9865  
9870  
9875  
9880  
9885  
9890  
9895  
9900  
9905  
9910  
9915  
9920  
9925  
9930  
9935  
9940  
9945  
9950  
9955  
9960  
9965  
9970  
9975  
9980  
9985  
9990  
9995  
10000  
10005  
10010  
10015  
10020  
10025  
10030  
10035  
10040  
10045  
10050  
10055  
10060  
10065  
10070  
10075  
10080  
10085  
10090  
10095  
10100  
10105  
10110  
10115  
10120  
10125  
10130  
10135  
10140  
10145  
10150  
10155  
10160  
10165  
10170  
10175  
10180  
10185  
10190  
1

selecting the delegator from a displayed list of delegators. The delegate may also enter the role(s) of the delegator that the delegate would like to assume, along with a confirmation code. The Web site may hash the confirmation code and provide the hashed results, along with the identities of the delegate and the requested role(s) to DSP 208, where they are received. DSP 208 stores the request and the hash of the confirmation code in database 214.

The delegate provides the confirmation code to the delegator. As was the case above, the confirmation code may be provided to the delegator by hand, electronic mail, or some other secure method that is independent of the delegation processes described herein.

The delegator may request, e.g., via a DSP Web site (not shown), outstanding delegation requests that relate to the delegator. That is, the delegator may ask DSP 208 who (which delegates) have requested roles of the delegator and which roles have been requested. DSP 208 receives the request from the delegator and provides the delegator with a list of the outstanding delegation requests. The list may include the requesting delegates and the role(s) that they have requested. Along with providing the list, DSP 208

requests that the delegator approve of the outstanding delegation request of the delegate.

To approve of the outstanding delegation request from the delegate, the delegator provides the confirmation code to DSP 208, along with the delegator's digital credential. DSP 208 receives the confirmation code and the digital credential. DSP 208 checks a hash of the confirmation code against a stored hash of the confirmation code and the digital credential of the delegator against a stored digital credential of the delegator. If both match, DSP 208 approves the outstanding delegation credential request of the delegate and stores the approval in database 214.

Process 248 reduces the problem of name similarity and name collision in secured communications. That is, use of a confirmation code, along with the digital credentials, provides a back-up identifier for the user.

In other embodiments, the confirmation code could be generated by the DSP Web site instead of by the delegator. The delegator could send the actual confirmation code instead of the hash of the confirmation code. There could be a time-out on the confirmation code so that if the confirmation code is not entered within a predetermined period of time, the confirmation code is invalidated. The

delegate could store the delegation information instead of storing it on DSP 208.

Processes 216, 230 and 248 are not limited to use with the hardware of Fig. 4; they may find applicability in any computing or processing environment. Processes 216, 230 and 248 may be implemented in hardware, software, or a combination of the two. Processes 216, 230 and 248 may be implemented in one or more computer programs executing on programmable computers that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and one or more output devices. Program code may be applied to data entered using an input device to perform processes 216, 230 and 248 and to generate output information. The output information may be applied to one or more output devices.

Each such program may be implemented in a high level procedural or object-oriented programming language to communicate with a computer system. However, the programs can be implemented in assembly or machine language. The language may be a compiled or an interpreted language.

Each computer program may be stored on an article of manufacture, e.g., a storage medium, such as a CD-ROM, hard

disk, or magnetic diskette, that is readable by a general or special purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform processes 216, 230 and 248.

5 Processes 216, 230 and 248 may also be implemented as a computer-readable storage medium, configured with a computer program, where, upon execution, instructions in the computer program cause the computer to operate in accordance with processes 216, 230 and 248.

10 The invention has been described with reference to a variety of embodiments. These and other embodiments not specifically described herein are within the scope of the following claims.

15 What is claimed is: